Exemplo de configuração de ASA/PIX com RIP

Contents

Introduction

Este documento explica como configurar o Cisco ASA para aprender rotas por meio do Routing Information Protocol (RIP), executar autenticação e redistribuição.

Consulte o PIX/ASA 8.X: Configuração do EIGRP no Cisco Adaptive Security Appliance (ASA) para obter mais informações sobre a configuração do EIGRP.

Observação: esta configuração de documento é baseada na versão 2 do RIP.

Observação: o roteamento assimétrico não é suportado no ASA/PIX.

Prerequisites

Requirements

Certifique-se de atender a estes requisitos antes de tentar esta configuração:

- O Cisco ASA/PIX deve executar a versão 7.x ou posterior.
- RIP não é suportado no modo multicontexto; ele é suportado somente em modo único.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco 5500 Series Adaptive Security Appliance (ASA) que executa a versão de software 8.0 e posterior.
- Software Cisco Adaptive Security Device Manager (ASDM) versão 6.0 e posterior.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Produtos Relacionados

As informações neste documento também se aplicam ao Cisco 500 Series PIX Firewall que executa o software versão 8.0 e posterior.

Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Informações de Apoio

O RIP é um protocolo de roteamento de vetor de distância que usa a contagem de saltos como métrica para a seleção do caminho. Quando o RIP é ativado em uma interface, a interface troca broadcasts do RIP com dispositivos vizinhos para aprender e anunciar dinamicamente rotas.

O Security Appliance suporta RIP versão 1 e RIP versão 2. O RIP versão 1 não envia a máscara de sub-rede com a atualização de roteamento. O RIP versão 2 envia a máscara de sub-rede com a atualização de roteamento e suporta máscaras de sub-rede de comprimento variável. Além disso, o RIP versão 2 suporta autenticação de vizinhos quando atualizações de roteamento são trocadas. Essa autenticação garante que o Security Appliance receba informações de roteamento confiáveis de uma origem confiável.

Limitações:

1. O Security Appliance não pode passar atualizações RIP entre interfaces.
2. O RIP Versão 1 não suporta VLSM (Variable-Length Subnet Mask).
3. O RIP tem uma contagem máxima de saltos de 15. Uma rota com uma contagem de saltos superior a 15 é considerada inalcançável.
4. A convergência do RIP é relativamente lenta em comparação a outros protocolos de roteamento.
5. Você só pode ativar um único processo RIP no Security Appliance.

Observação: essas informações se aplicam somente ao RIP versão 2:

1. Se você usar a autenticação de vizinhos, a chave de autenticação e o ID da chave devem ser os mesmos em todos os dispositivos vizinhos que fornecem atualizações RIP versão 2 à interface.
2. Com o RIP versão 2, o Security Appliance transmite e recebe atualizações de rota padrão com o uso do endereço multicast 224.0.0.9. No modo passivo, ele recebe atualizações de rota nesse endereço.
3. Quando o RIP versão 2 é configurado em uma interface, o endereço multicast 224.0.0.9 é registrado nessa interface. Quando uma configuração RIP versão 2 é removida de uma interface, esse endereço multicast não é registrado.

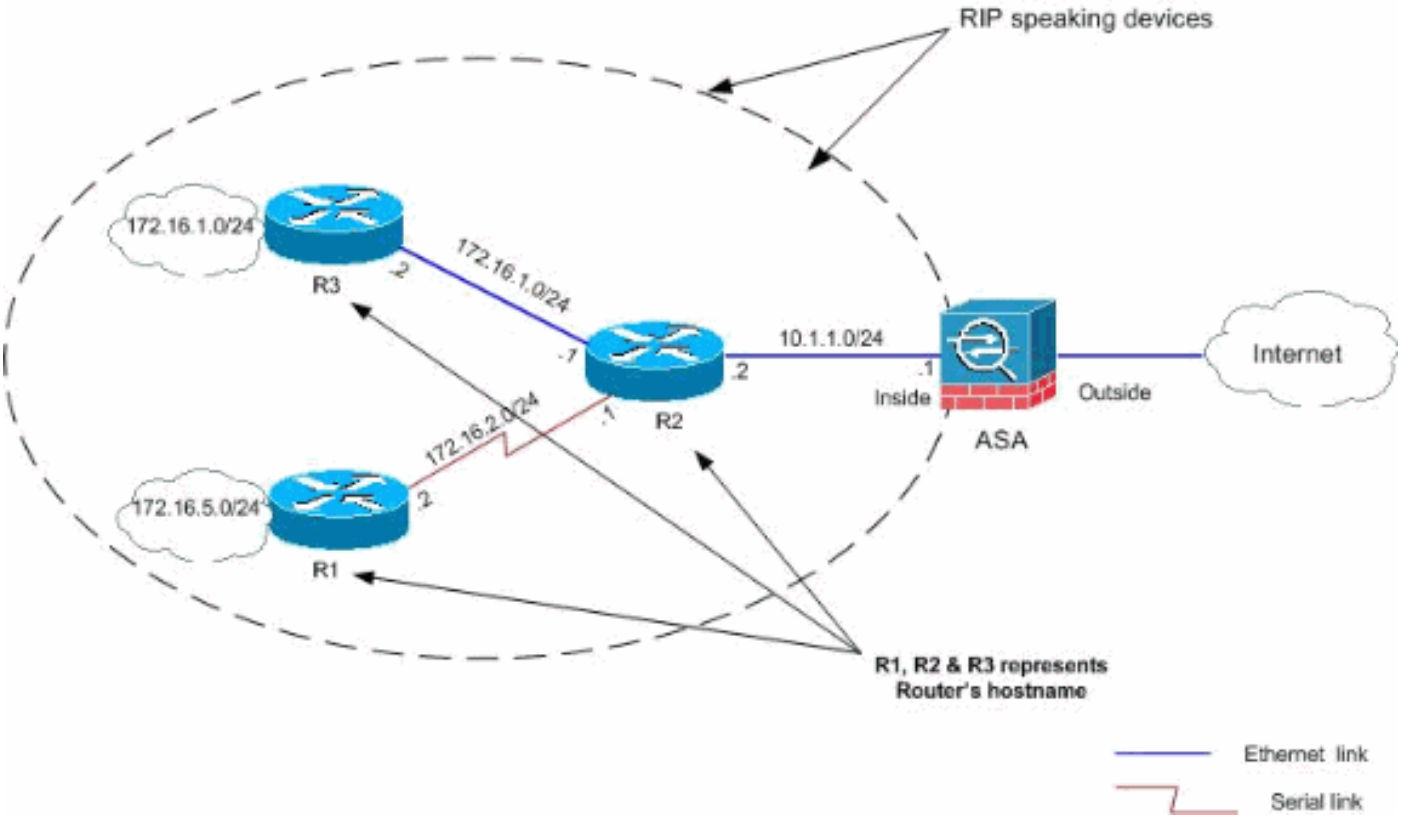
Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Nota:Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Configurações

Este documento utiliza as seguintes configurações:

- Configuração do ASDM
- Configurar a autenticação do RIP

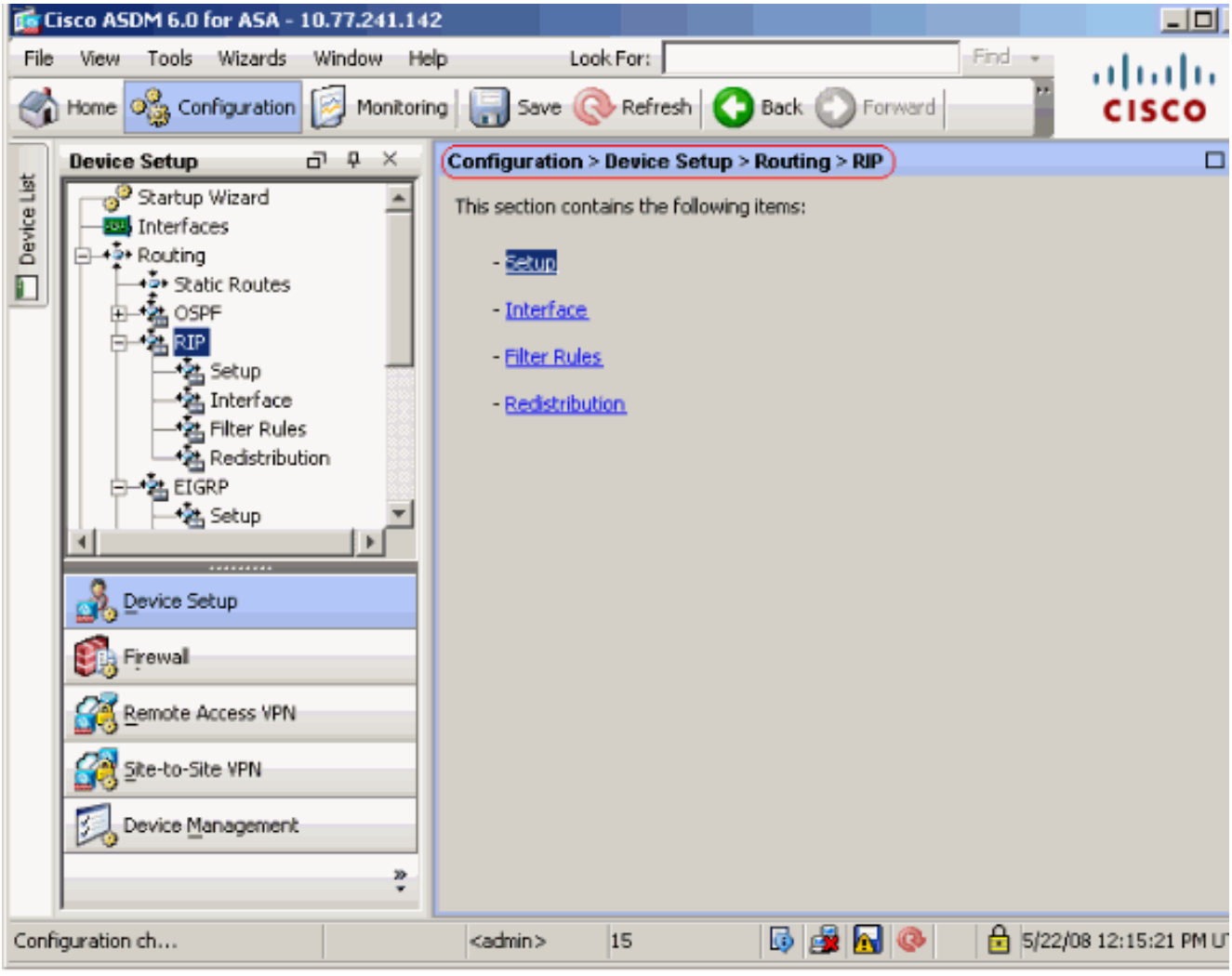
- Configuração do Cisco ASA CLI
- Configuração da CLI do Cisco IOS Router (R2)
- Configuração do Cisco IOS Router (R1) CLI
- Configuração da CLI do Cisco IOS Router (R3)

Configuração do ASDM

O Adaptive Security Device Manager (ASDM) é um aplicativo baseado em navegador usado para configurar e monitorar o software em dispositivos de segurança. O ASDM é carregado do Security Appliance e usado para configurar, monitorar e gerenciar o dispositivo. Você também pode usar o ASDM Launcher (Windows® somente) para iniciar o aplicativo ASDM mais rápido que o miniaplicativo Java. Esta seção descreve as informações necessárias para configurar os recursos descritos neste documento com o ASDM.

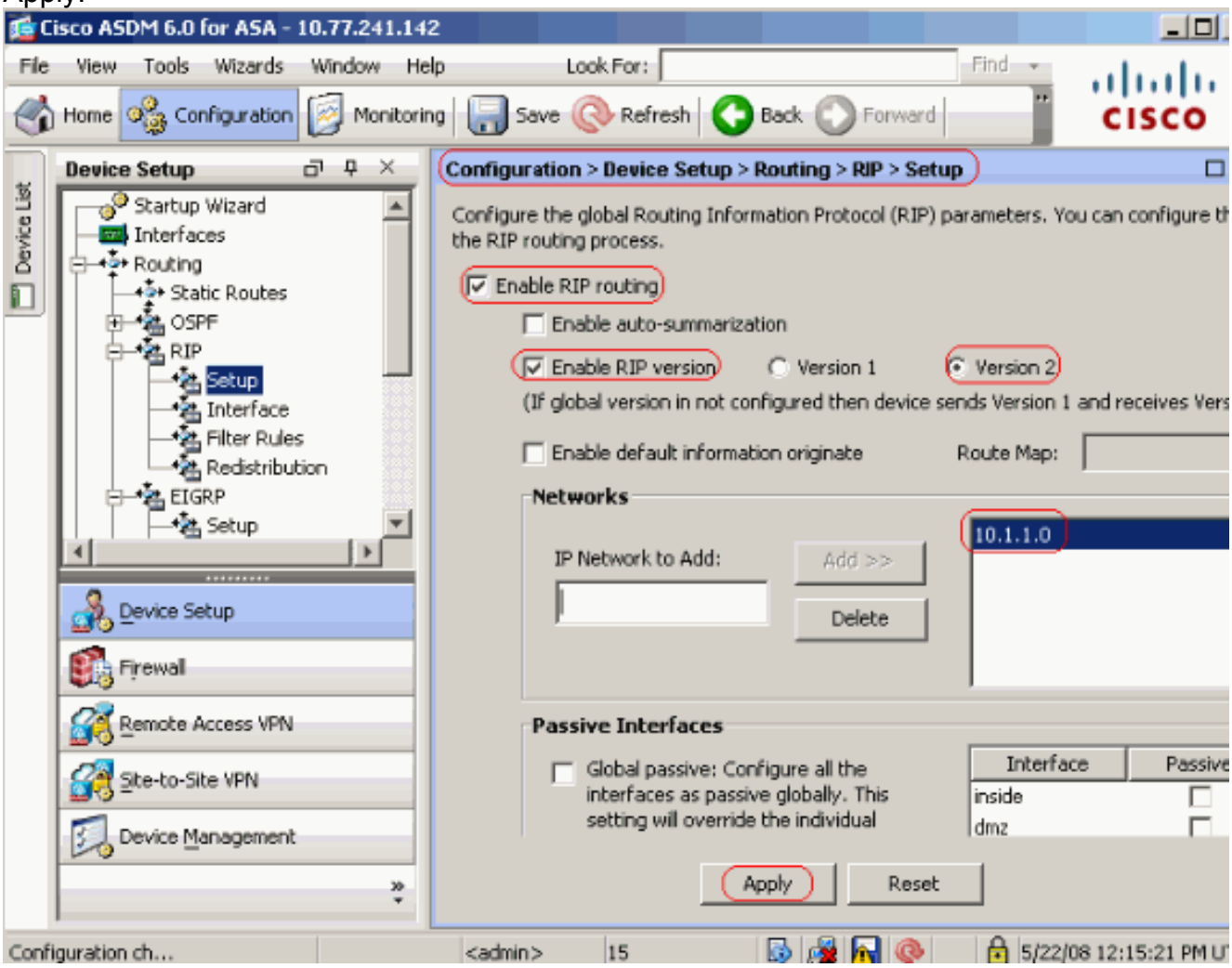
Conclua estes passos para configurar o RIP no Cisco ASA:

1. Faça login no Cisco ASA com ASDM.
2. Escolha **Configuration > Device Setup > Routing > RIP** na interface ASDM, como mostrado na captura de
tela.



3. Escolha **Configuration > Device Setup > Routing > RIP > Setup** para ativar o roteamento RIP conforme mostrado.Escolha a caixa de seleção **Ativar roteamento RIP**.Escolha a caixa de seleção **Ativar versão do RIP** com o botão de opção **Versão 2**.Na guia **Redes**, adicione a rede **10.1.1.0**.Clique em

Apply.



CamposAtivar o roteamento RIP—Marque essa caixa de seleção para ativar o roteamento RIP no Security Appliance. Quando você ativa o RIP, ele é ativado em todas as interfaces. Se você marcar essa caixa de seleção, isso também ativará os outros campos neste painel. Desmarque essa caixa de seleção para desabilitar o roteamento RIP no Security Appliance.Habilitar sumarização automática—Desmarque essa caixa de seleção para desabilitar a sumarização automática de rotas. Marque essa caixa de seleção para reativar a sumarização automática de rotas. O RIP Versão 1 sempre usa a sumarização automática. Não é possível desativar a sumarização automática para o RIP Versão 1. Se você usar o RIP Versão 2, poderá desativar a sumarização automática se desmarcar essa caixa de seleção. Desabilite a sumarização automática se você precisar executar o roteamento entre sub-redes desconectadas. Quando a sumarização automática está desativada, as sub-redes são anunciadas.Ativar versão do RIP — Marque essa caixa de seleção para especificar a versão do RIP usada pelo Security Appliance. Se essa caixa de seleção estiver desmarcada, o Security Appliance enviará atualizações do RIP Versão 1 e aceitará atualizações do RIP Versão 1 e Versão 2. Essa configuração pode ser substituída em uma base por interface no painel Interface.Versão 1—Especifica que o Security Appliance somente envia e recebe atualizações do RIP Versão 1. Todas as atualizações da versão 2 recebidas são descartadas.Versão 2—Especifica que o Security Appliance somente envia e recebe atualizações do RIP Versão 2. Todas as atualizações da versão 1 recebidas são descartadas.Ativar a origem de informações padrão — Marque essa caixa de seleção para gerar uma rota padrão no processo de roteamento RIP. Você pode configurar um mapa de rotas que deve ser satisfeito antes que a rota padrão possa ser gerada.Route-map—Insira o

nome do mapa de rota para se aplicar. O processo de roteamento gera a rota padrão se o mapa de rotas for satisfeito.Rede IP a adicionar—Define uma rede para o processo de roteamento RIP. O número de rede especificado não deve conter nenhuma informação de sub-rede. Não há limite para o número de redes que você pode adicionar à configuração do Security Appliance. As atualizações de roteamento RIP são enviadas e recebidas somente por meio de interfaces nas redes especificadas. Além disso, se a rede de uma interface não for especificada, a interface não será anunciada em nenhuma atualização do RIP.Adicionar—Clique neste botão para adicionar a rede especificada à lista de redes.Excluir—Clique nesse botão para remover a rede selecionada da lista de redes.Configurar interfaces como passivas globalmente — Marque essa caixa de seleção para definir todas as interfaces no Security Appliance para o modo RIP passivo. O Security Appliance ouve broadcasts de roteamento RIP em todas as interfaces e usa essas informações para preencher as tabelas de roteamento, mas não transmite atualizações de roteamento. Use a tabela Interfaces Passivas para definir interfaces específicas para RIP passivo.Tabela de interfaces passivas—Lista as interfaces configuradas no Security Appliance. Marque a caixa de seleção na coluna Passivo para as interfaces que deseja operar no modo passivo. As outras interfaces ainda enviam e recebem broadcasts RIP.

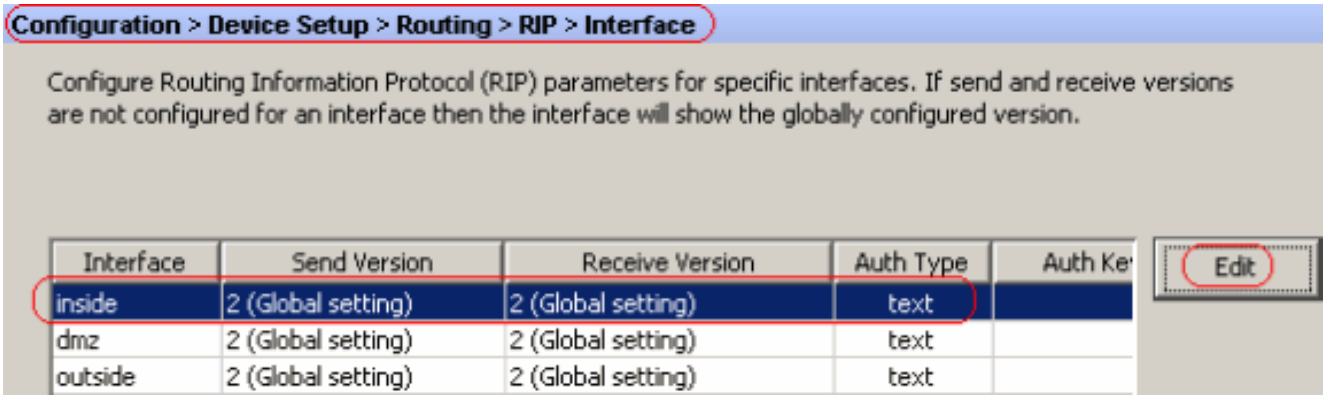
Configurar a autenticação do RIP

O Cisco ASA suporta a autenticação MD5 de atualizações de roteamento do protocolo de roteamento RIP v2. O MD5 keyed digest em cada pacote RIP impede a introdução de mensagens de roteamento não autorizadas ou falsas de fontes não aprovadas. A adição de autenticação às mensagens do RIP garante que os roteadores e o Cisco ASA aceitem apenas mensagens de roteamento de outros dispositivos de roteamento configurados com a mesma chave pré-compartilhada. Sem essa autenticação configurada, se você introduzir outro dispositivo de roteamento com informações de rota diferentes ou contrárias na rede, as tabelas de roteamento em seus roteadores ou no Cisco ASA podem ficar corrompidas e um ataque de negação de serviço pode ocorrer. Quando você adiciona autenticação às mensagens do RIP enviadas entre seus dispositivos de roteamento, que inclui o ASA, ele evita a adição acidental ou proposital de outro roteador à rede e qualquer problema.

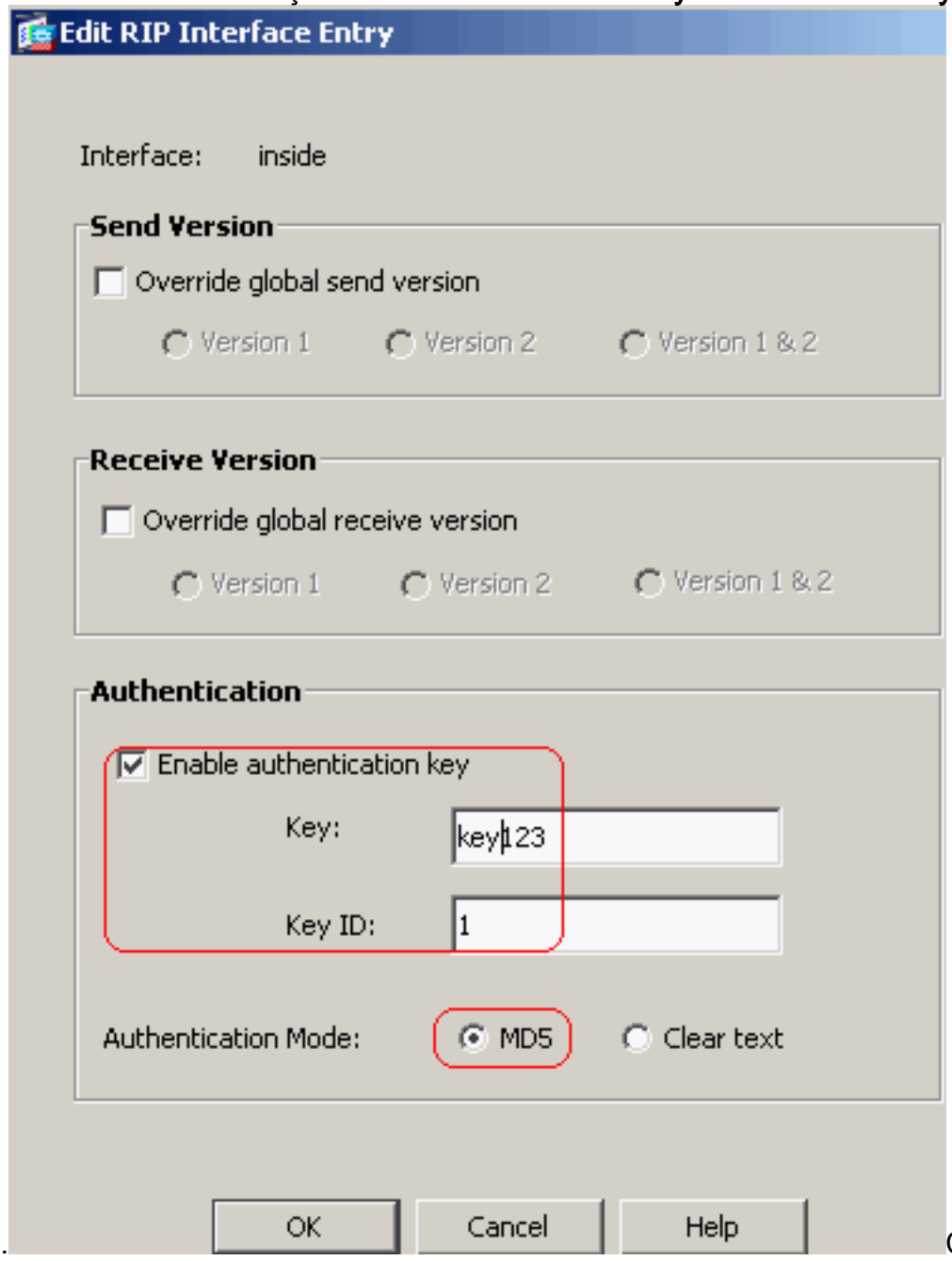
A autenticação de rota RIP é configurada por interface. Todos os vizinhos RIP em interfaces configuradas para autenticação de mensagem RIP devem ser configurados com o mesmo modo de autenticação e chave.

Conclua estes passos para habilitar a autenticação MD5 do RIP no Cisco ASA.

1. No ASDM, escolha **Configuration > Device Setup > Routing > RIP > Interface** e escolha a interface interna com o mouse. Clique em **Editar**.



2. Escolha a caixa de seleção **Enable authentication key** e insira o valor **Key** e **Key** ID.



Clique em **OK e, em seguida, em Apply**.

Configuração do Cisco ASA CLI

Cisco ASA

```
ciscoasa#show running-config
: Saved
:
ASA Version 8.0(2)
!
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!

!--- Inside interface configuration interface
Ethernet0/1 nameif inside security-level 100 ip address
10.1.1.1 255.255.255.0 !--- RIP authentication is
configured on the inside interface. rip authentication
mode md5
 rip authentication key




!

!--- Output Suppressed !--- Outside interface
configuration interface Ethernet0/2 nameif outside
security-level 0 ip address 192.168.1.2 255.255.255.0 !-
-- RIP Configuration router rip
 network 10.0.0.0
 version 2

!--- This is the static default gateway configuration in
!--- order to reach the Internet. route outside 0.0.0.0
0.0.0.0 192.168.1.1 1
```

Configuração da CLI do Cisco IOS Router (R2)

Roteador Cisco IOS (R2)

```
interface Ethernet0
 ip address 10.1.1.2 255.255.255.0
 ip rip authentication mode md5
 ip rip authentication key-chain 1

!
router rip
 version 2
 network 10.0.0.0
 network 172.16.0.0
 no auto-summary
```

Configuração do Cisco IOS Router (R1) CLI

Roteador Cisco IOS (R1)

```
router rip
 version 2
 network 172.16.0.0
 no auto-summary
```

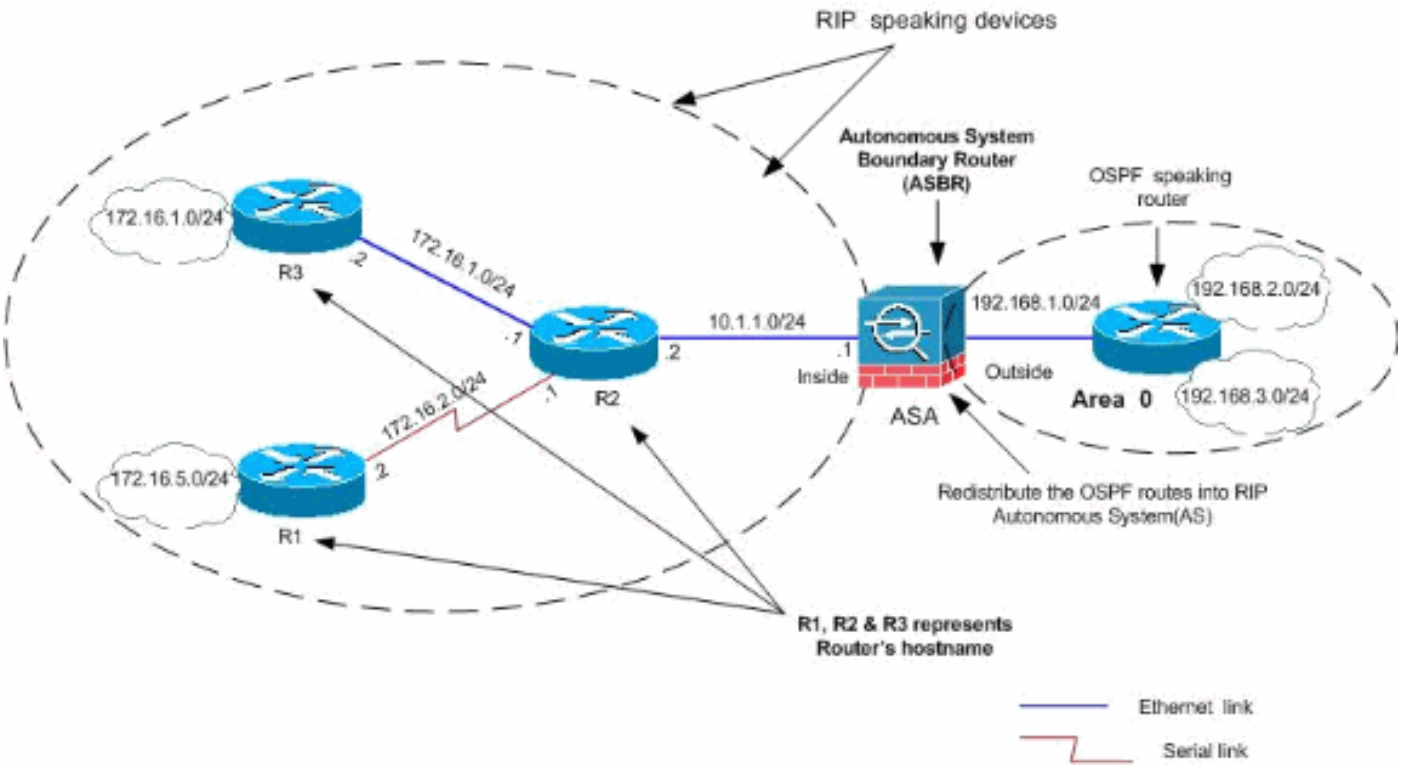
Configuração da CLI do Cisco IOS Router (R3)

Roteador Cisco IOS (R3)
router rip version 2 network 172.16.0.0 no auto-summary

Redistribuir em RIP com ASA

Você pode redistribuir rotas dos processos de roteamento OSPF, EIGRP, estático e conectado no processo de roteamento RIP.

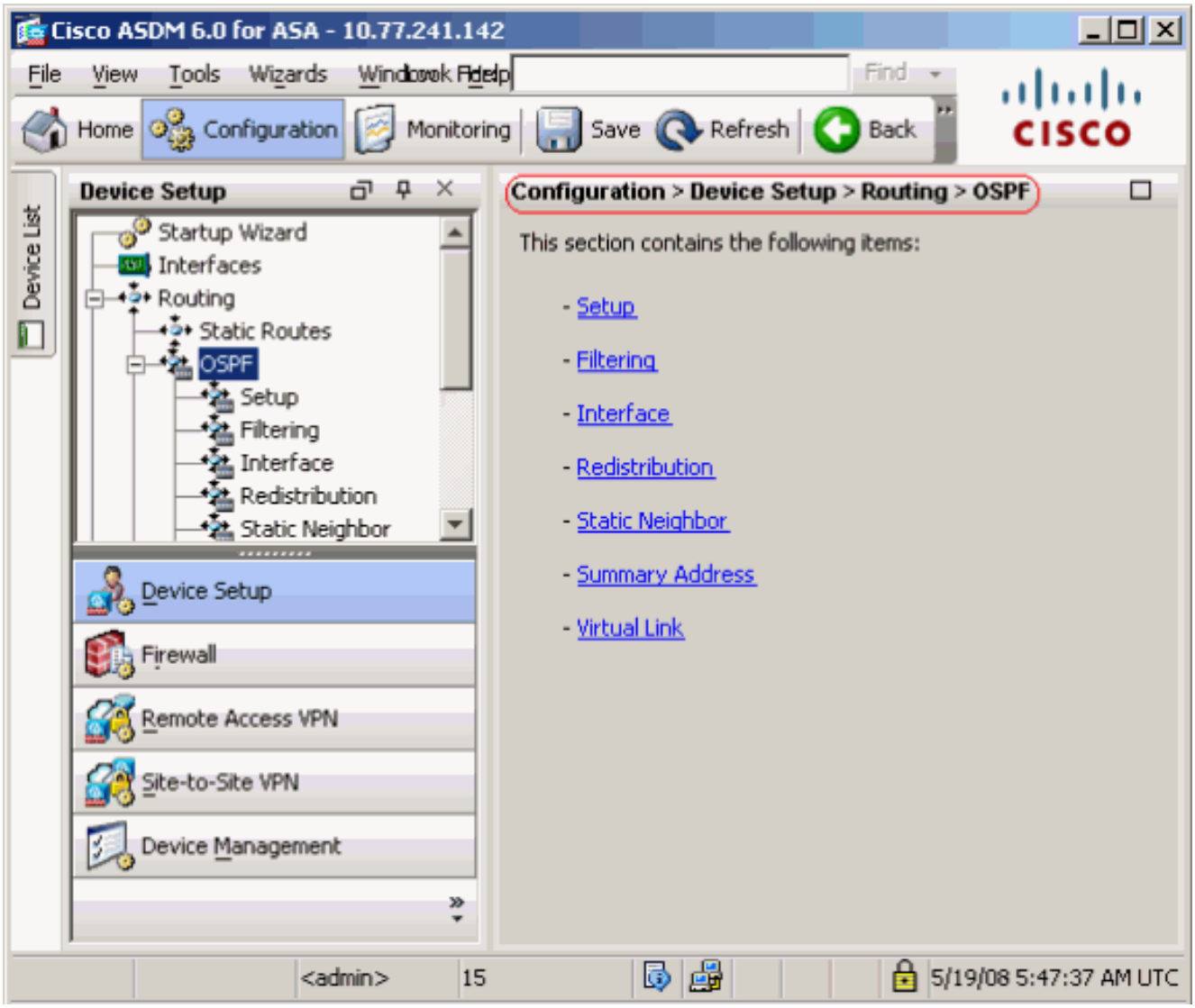
Neste exemplo, a redistribuição das rotas OSPF no RIP com o diagrama de rede é mostrada:



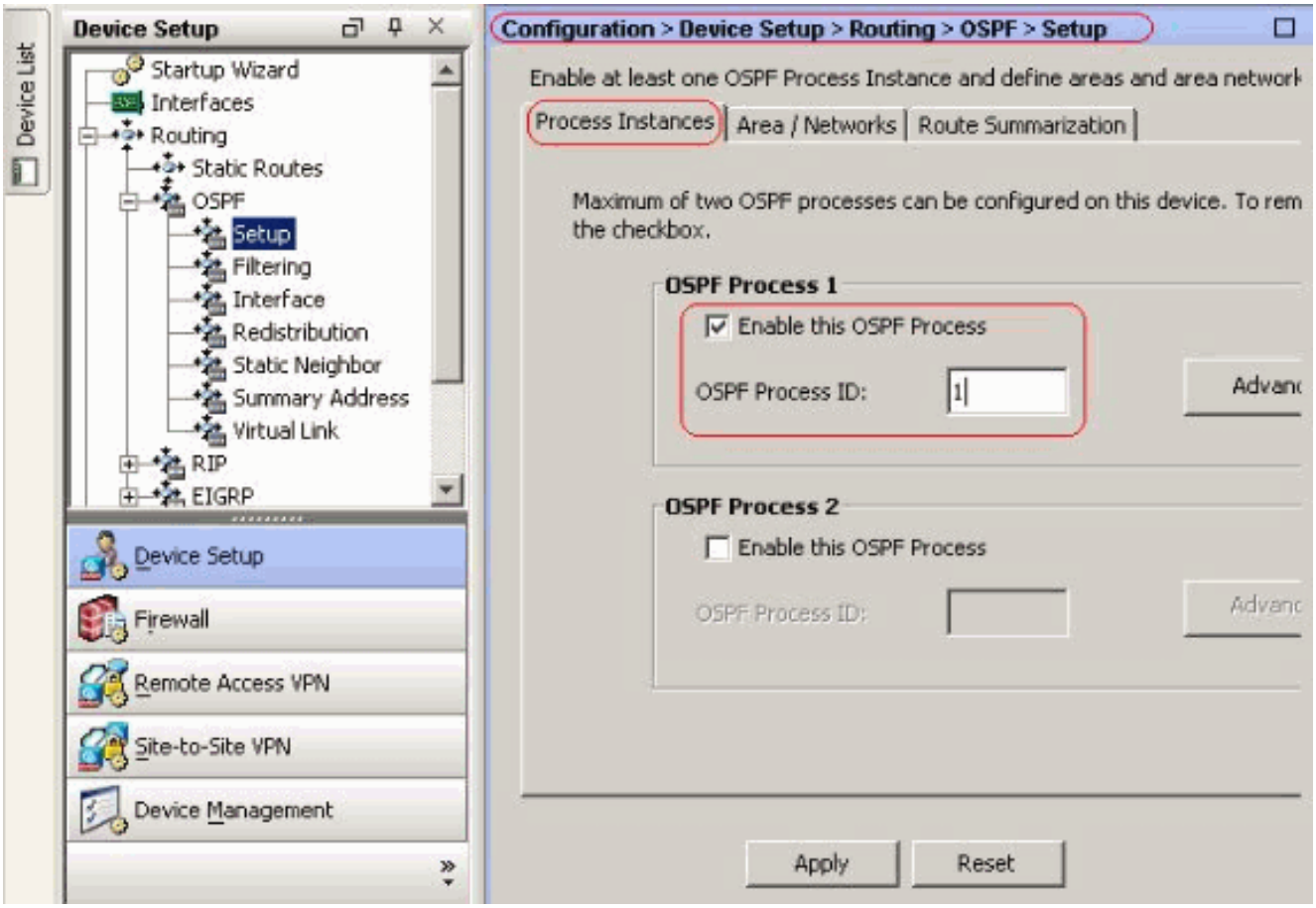
Configuração do ASDM

Conclua estes passos:

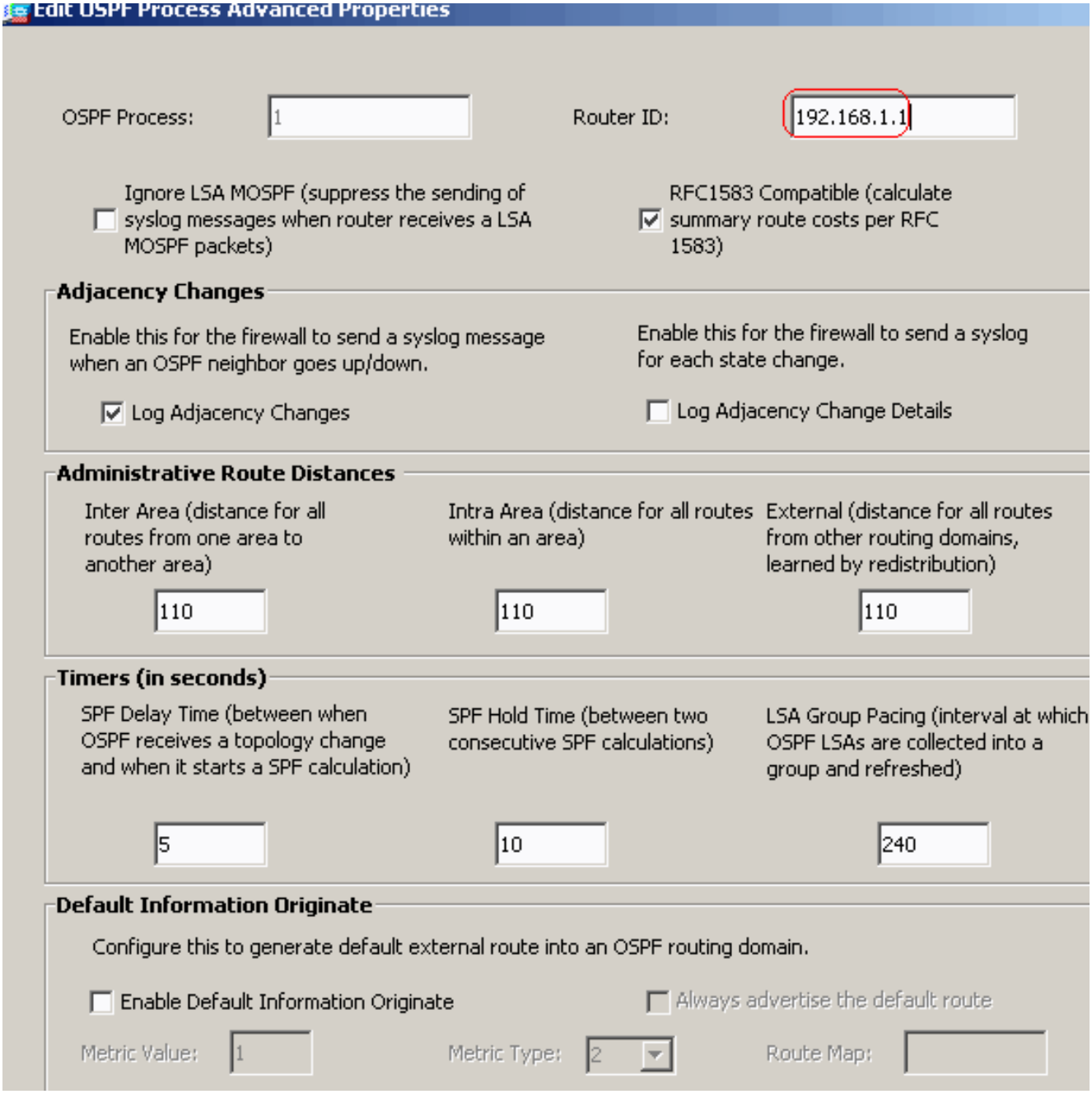
1. **Configuração do OSPF**Escolha **Configuration > Device Setup > Routing > OSPF** na interface do ASDM, como mostrado na captura de tela.



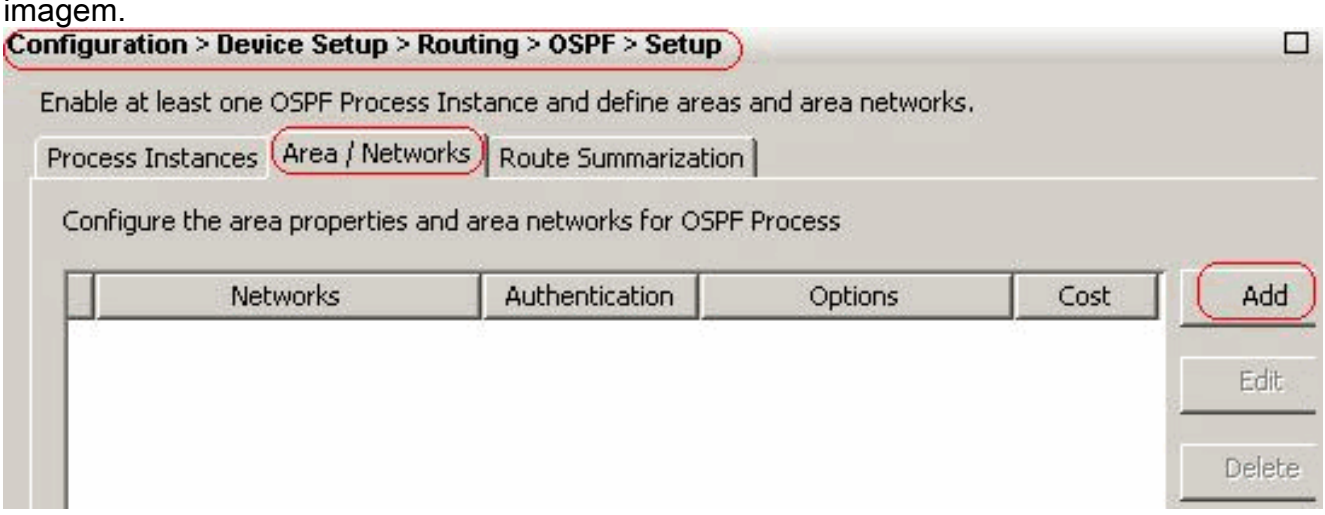
Ative o processo de roteamento OSPF na guia **Setup > Process Instances**, como mostrado na captura de tela. Neste exemplo, o processo de ID do OSPF é **1**.



Clique em **Advanced** na guia **Setup > Process Instances** para configurar parâmetros do processo de roteamento OSPF avançados opcionais. Você pode editar configurações específicas do processo, como ID do roteador, Alterações de adjacência, Distâncias de rota administrativa, Temporizadores e Configurações de origem das informações padrão.

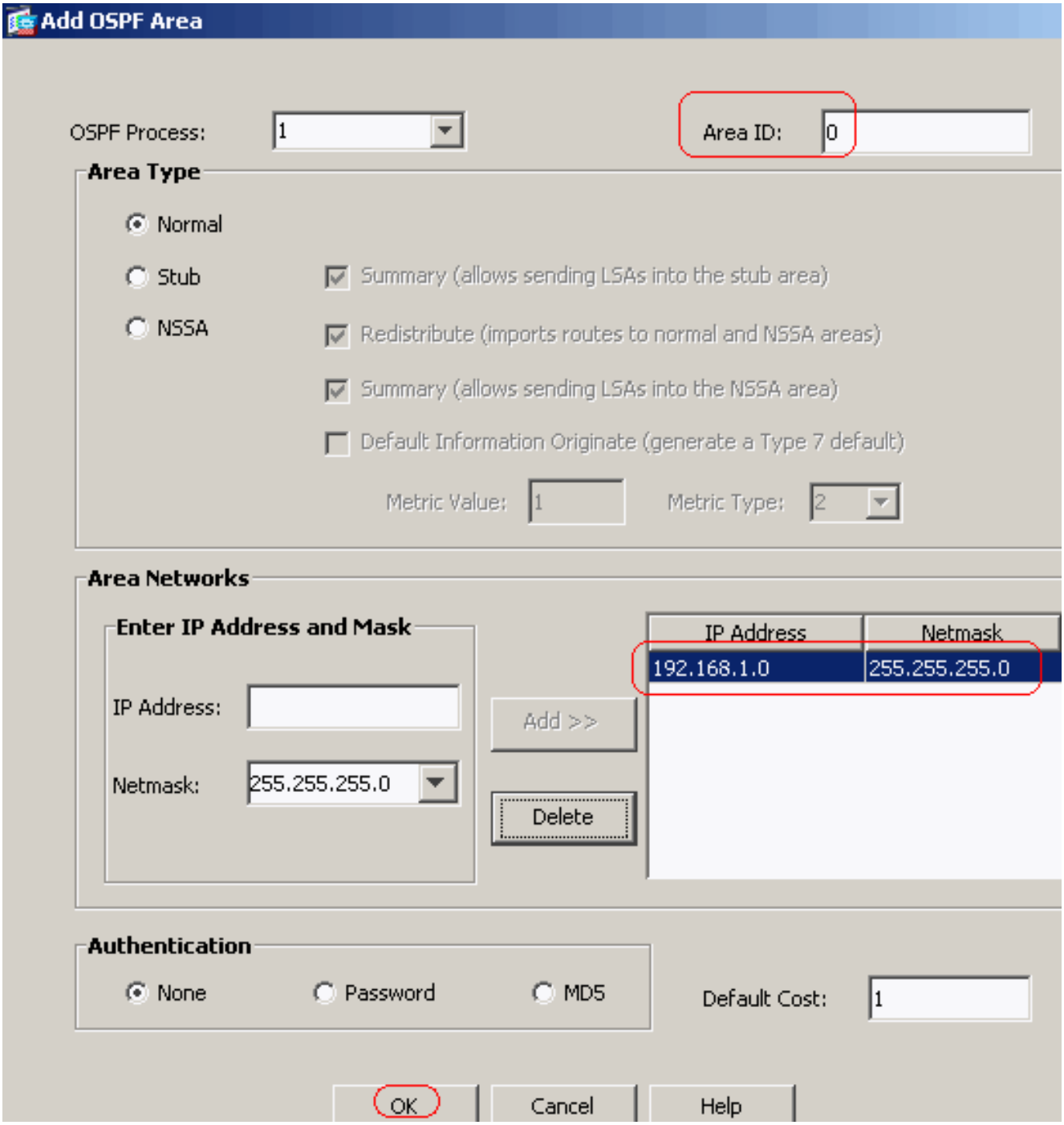


Click **OK**.Depois de concluir as etapas anteriores, defina as redes e as interfaces que participam do roteamento OSPF na guia **Setup > Area/Networks**. Clique em **Adicionar** conforme mostrado nesta
imagem.

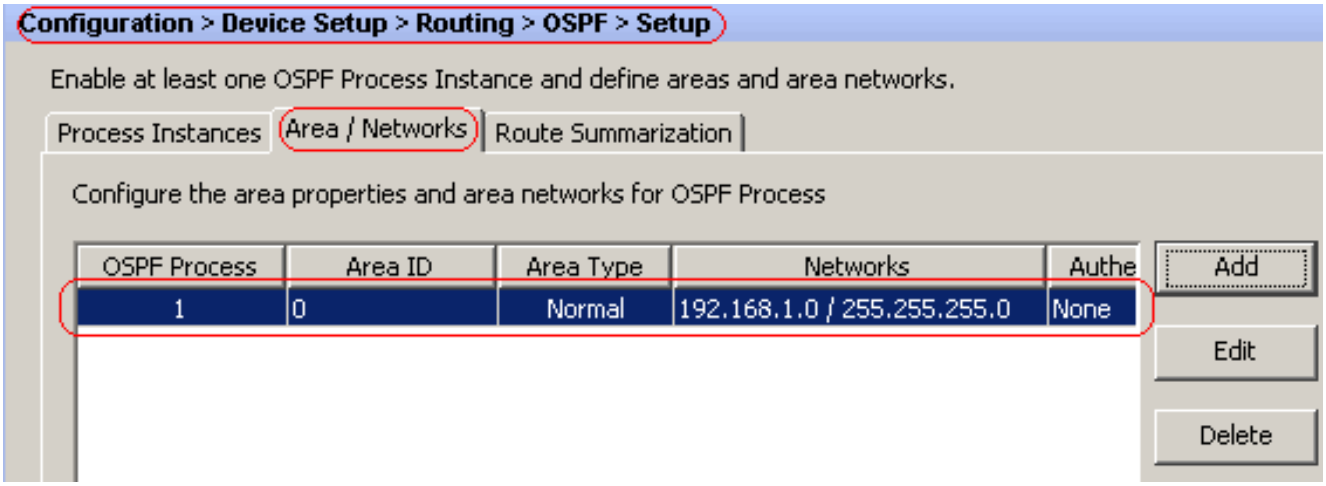


Esta tela é exibida. Neste exemplo, a única rede que adicionamos é a rede externa

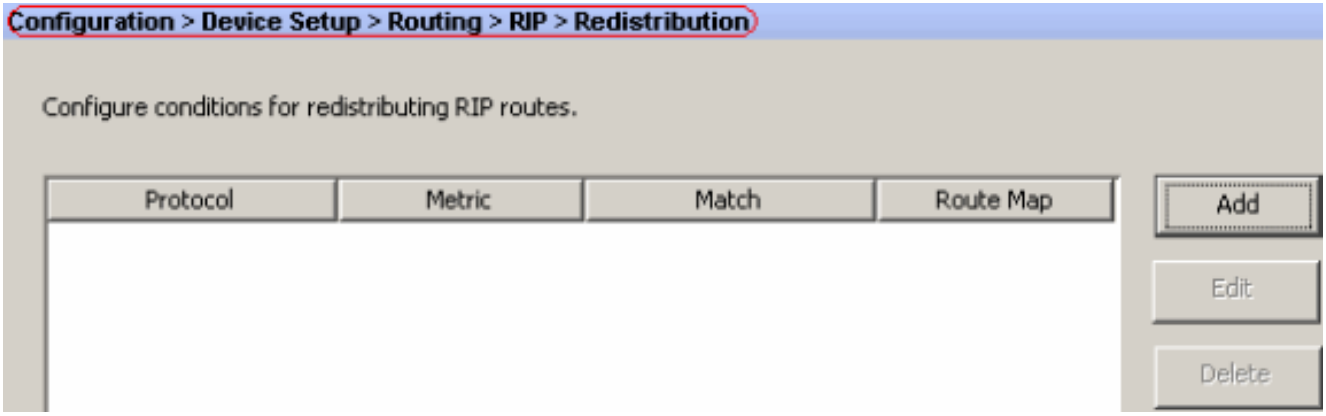
(192.168.1.0/24), já que o OSPF está ativado apenas na interface externa.**Observação:** somente as interfaces com um endereço IP que se enquadram nas redes definidas participam do processo de roteamento
OSPF.



Click **OK**.Clique em
Apply.

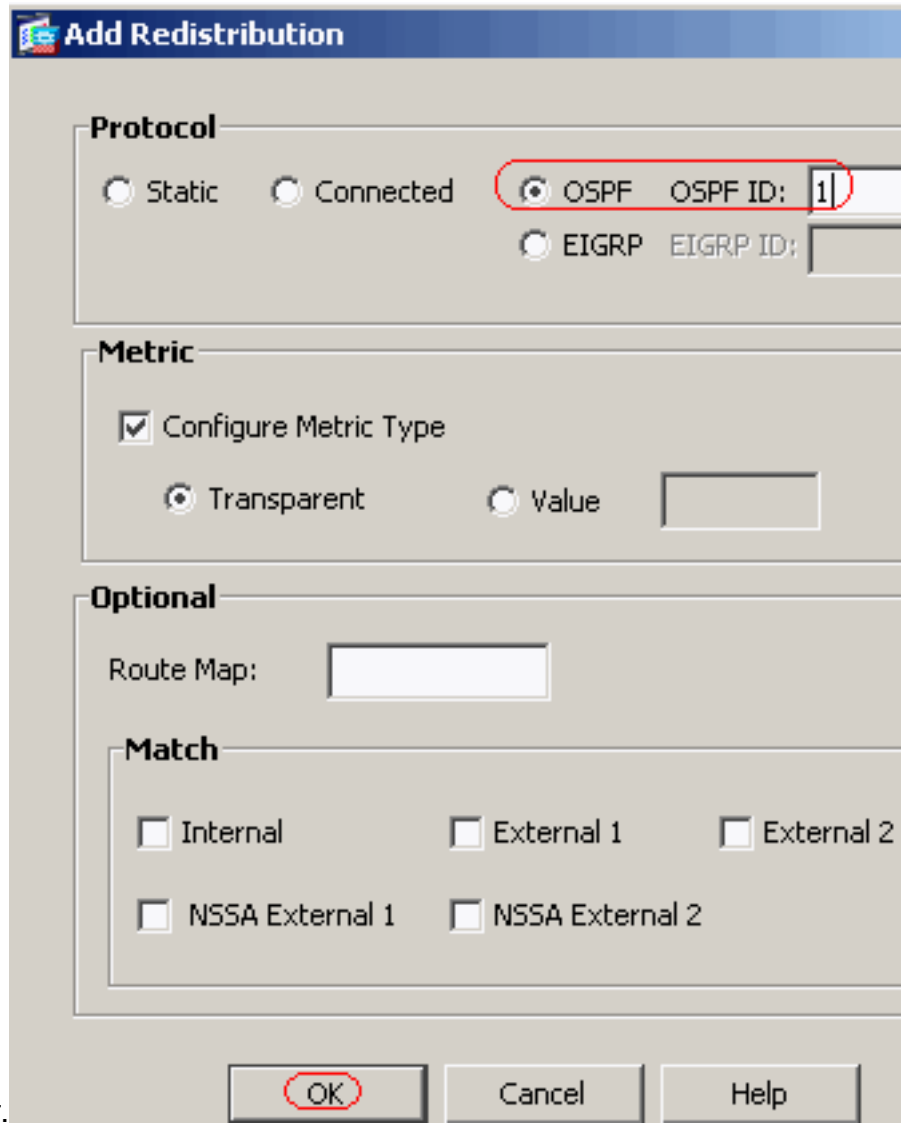


2. Escolha **Configuration > Device Setup > Routing > RIP > Redistribution > Add** para redistribuir rotas OSPF no
RIP.



3. Clique em **OK e, em seguida, em**

Apply.



Configuração de CLI equivalente

Configuração CLI do ASA para Redistribuir OSPF em RIP AS
router rip network 10.0.0.0 **redistribute ospf 1 metric transparent** version 2 ! router ospf 1 router-id 192.168.1.1 network 192.168.1.0 255.255.255.0 area 0 area 0 log-adj-changes

Você pode ver a tabela de roteamento do vizinho Cisco IOS Router(R2) após redistribuir rotas OSPF no RIP AS.

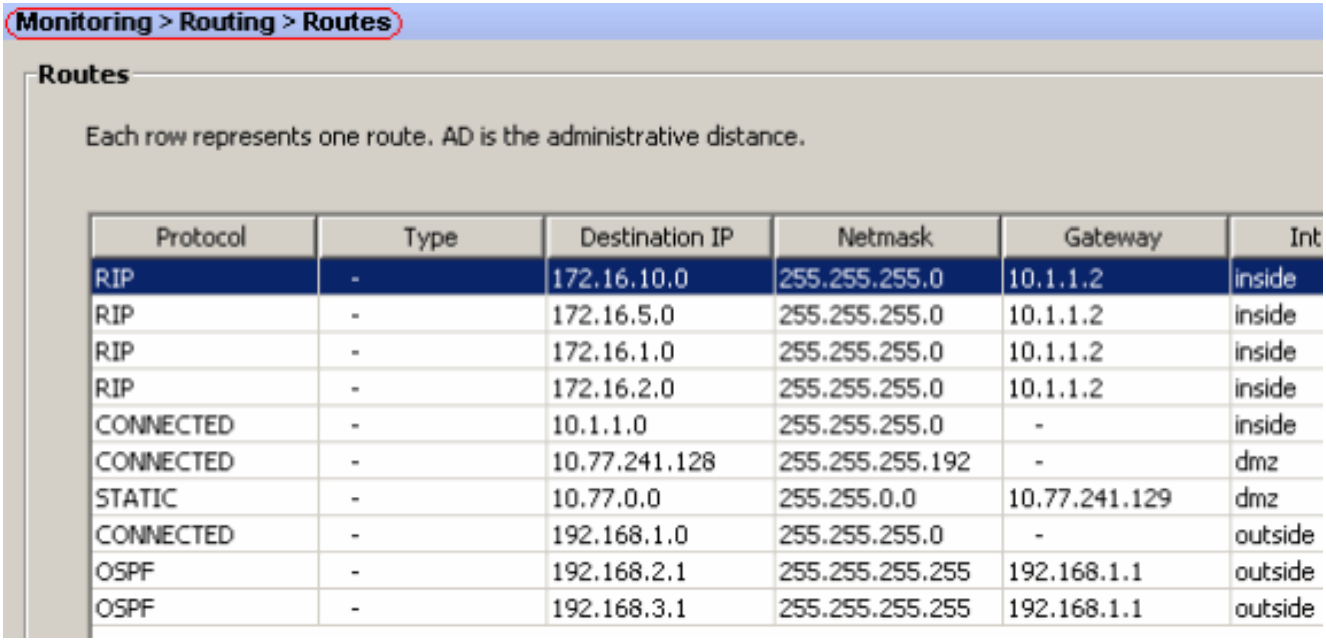
```
R2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
```

```
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default, U - per-user static route
        o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 4 subnets
R       172.16.10.0 [120/1] via 172.16.1.2, 00:00:25, Ethernet1
R       172.16.5.0 [120/1] via 172.16.2.2, 00:00:20, Serial1
C       172.16.1.0 is directly connected, Ethernet1
C       172.16.2.0 is directly connected, Serial1
     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       10.1.1.0/24 is directly connected, Ethernet0
R       10.77.241.128/26 [120/1] via 10.1.1.1, 00:00:06, Ethernet0
R    192.168.1.0/24 [120/1] via 10.1.1.1, 00:00:05, Ethernet0
     192.168.2.0/32 is subnetted, 1 subnets
R       192.168.2.1 [120/12] via 10.1.1.1, 00:00:05, Ethernet0
     192.168.3.0/32 is subnetted, 1 subnets
R       192.168.3.1 [120/12] via 10.1.1.1, 00:00:05, Ethernet0
!--- Redistributed route advertised by Cisco ASA
```

Verificar

Conclua estes passos para verificar sua configuração:

1. Você pode verificar a tabela de roteamento se navegar para **Monitoring > Routing > Routing**. Nesta captura de tela, você pode ver que as redes 172.16.1.0/24, 172.16.2.0/24, 172.16.5.0/24 e 172.16.10.0/24 são aprendidas através de R2 (10.1.1.2) com RIP.



Protocol	Type	Destination IP	Netmask	Gateway	Int
RIP	-	172.16.10.0	255.255.255.0	10.1.1.2	inside
RIP	-	172.16.5.0	255.255.255.0	10.1.1.2	inside
RIP	-	172.16.1.0	255.255.255.0	10.1.1.2	inside
RIP	-	172.16.2.0	255.255.255.0	10.1.1.2	inside
CONNECTED	-	10.1.1.0	255.255.255.0	-	inside
CONNECTED	-	10.77.241.128	255.255.255.192	-	dmz
STATIC	-	10.77.0.0	255.255.0.0	10.77.241.129	dmz
CONNECTED	-	192.168.1.0	255.255.255.0	-	outside
OSPF	-	192.168.2.1	255.255.255.255	192.168.1.1	outside
OSPF	-	192.168.3.1	255.255.255.255	192.168.1.1	outside

2. Na CLI, você pode usar o comando **show route** para obter a mesma saída.

```
ciscoasa#show route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
```

```
Gateway of last resort is not set

R    172.16.10.0 255.255.255.0 [120/2] via 10.1.1.2, 0:00:10, inside
R    172.16.5.0 255.255.255.0 [120/2] via 10.1.1.2, 0:00:10, inside
R    172.16.1.0 255.255.255.0 [120/1] via 10.1.1.2, 0:00:10, inside
R    172.16.2.0 255.255.255.0 [120/1] via 10.1.1.2, 0:00:10, inside
C    10.1.1.0 255.255.255.0 is directly connected, inside
C    10.77.241.128 255.255.255.192 is directly connected, dmz
S    10.77.0.0 255.255.0.0 [1/0] via 10.77.241.129, dmz
C    192.168.1.0 255.255.255.0 is directly connected, outside
O    192.168.2.1 255.255.255.255 [110/11] via 192.168.1.1, 0:34:46, outside
O    192.168.3.1 255.255.255.255 [110/11] via 192.168.1.1, 0:34:46, outside
ciscoasa#
```

Troubleshoot

Esta seção inclui informações sobre comandos debug que podem ser úteis para solucionar problemas do OSPF.

Comandos para Troubleshooting

A Output Interpreter Tool (somente clientes registrados) (OIT) oferece suporte a determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

Nota:Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos debug.

- **debug rip events** —Habilita a depuração de eventos RIP

```
ciscoasa#debug rip events
rip_route_adjust for inside coming up
RIP: sending request on inside to 224.0.0.9
RIP: received v2 update from 10.1.1.2 on inside
     172.16.1.0255.255.255.0 via 0.0.0.0 in 1 hops
     172.16.2.0255.255.255.0 via 0.0.0.0 in 1 hops
     172.16.5.0255.255.255.0 via 0.0.0.0 in 2 hops
     172.16.10.0255.255.255.0 via 0.0.0.0 in 2 hops
RIP: Update contains 4 routes
RIP: received v2 update from 10.1.1.2 on inside
     172.16.1.0255.255.255.0 via 0.0.0.0 in 1 hops
     172.16.2.0255.255.255.0 via 0.0.0.0 in 1 hops
     172.16.5.0255.255.255.0 via 0.0.0.0 in 2 hops
     172.16.10.0255.255.255.0 via 0.0.0.0 in 2 hops
RIP: Update contains 4 routes
RIP: sending v2 flash update to 224.0.0.9 via dmz (10.77.241.142)
RIP: build flash update entries
        10.1.1.0 255.255.255.0 via 0.0.0.0, metric 1, tag 0
        172.16.1.0 255.255.255.0 via 0.0.0.0, metric 2, tag 0
        172.16.2.0 255.255.255.0 via 0.0.0.0, metric 2, tag 0
        172.16.5.0 255.255.255.0 via 0.0.0.0, metric 3, tag 0
        172.16.10.0 255.255.255.0 via 0.0.0.0, metric 3, tag 0
RIP: Update contains 5 routes
RIP: Update queued
RIP: sending v2 flash update to 224.0.0.9 via inside (10.1.1.1)
RIP: build flash update entries - suppressing null update
RIP: Update sent via dmz rip-len:112
RIP: sending v2 update to 224.0.0.9 via dmz (10.77.241.142)
RIP: build update entries
        10.1.1.0 255.255.255.0 via 0.0.0.0, metric 1, tag 0
        172.16.1.0 255.255.255.0 via 0.0.0.0, metric 2, tag 0
```

```
        172.16.2.0 255.255.255.0 via 0.0.0.0, metric 2, tag 0
        172.16.5.0 255.255.255.0 via 0.0.0.0, metric 3, tag 0
        172.16.10.0 255.255.255.0 via 0.0.0.0, metric 3, tag 0
        192.168.1.0 255.255.255.0 via 0.0.0.0, metric 1, tag 0
        192.168.2.1 255.255.255.255 via 0.0.0.0, metric 12, tag 0
        192.168.3.1 255.255.255.255 via 0.0.0.0, metric 12, tag 0
RIP: Update contains 8 routes
RIP: Update queued
RIP: sending v2 update to 224.0.0.9 via inside (10.1.1.1)
RIP: build update entries
        10.77.241.128 255.255.255.192 via 0.0.0.0, metric 1, tag 0
        192.168.1.0 255.255.255.0 via 0.0.0.0, metric 1, tag 0
        192.168.2.1 255.255.255.255 via 0.0.0.0, metric 12, tag 0
        192.168.3.1 255.255.255.255 via 0.0.0.0, metric 12, tag 0
RIP: Update contains 4 routes
RIP: Update queued
RIP: Update sent via dmz rip-len:172
RIP: Update sent via inside rip-len:92
RIP: received v2 update from 10.1.1.2 on inside
     172.16.1.0255.255.255.0 via 0.0.0.0 in 1 hops
     172.16.2.0255.255.255.0 via 0.0.0.0 in 1 hops
     172.16.5.0255.255.255.0 via 0.0.0.0 in 2 hops
     172.16.10.0255.255.255.0 via 0.0.0.0 in 2 hops
RIP: Update contains 4 routes
```

Informações Relacionadas

- Página de Suporte do Cisco 5500 Series Adaptive Security Appliance
- Página de suporte do Cisco 500 Series PIX
- PIX/ASA 8.X: Configuração do EIGRP no Cisco Adaptive Security Appliance (ASA)
- Suporte Técnico e Documentação - Cisco Systems